AN INVESTIGATION ON HASH BASED BIOMETRIC KEY AUTHENTICATION AND ASYMMETRIC CRYPTOGRAPHIC TECHNIQUES FOR SECURED DATA ACCESS IN CLOUD

A SYNOPSIS

Submitted by

K. MOHANA PRABHA

(Reg. No. 201506219)

in partial fulfillment for the award of the degree

of

DOCTOR OF PHILOSOPHY

DEPARTMENT OF COMPUTER APPLICATIONS

SCHOOL OF COMPUTING

KALASALINGAM ACADEMY OF RESEARCH AND EDUCATION

(DEEMED TO BE UNIVERSITY)

ANAND NAGAR, KRISHNANKOIL – 626126

TAMIL NADU, INDIA.

AUGUST 2022

AN INVESTIGATION ON HASH BASED BIOMETRIC KEY AUTHENTICATION AND ASYMMETRIC CRYPTOGRAPHIC TECHNIQUES FOR SECURED DATA ACCESS IN CLOUD

This Thesis comprises the research work carried out by K. Mohana Prabha under the supervision of Dr. S. Balamurali.

1. INTRODUCTION

Cloud computing presents a different source of applications and services through the internet-based computing to several users in a secured manner. Basically, cloud computing offers a regular structure for providing network access to software, shared data, infrastructure and platform resources. With the use of network access, cloud service interaction is achieved with minimum time utilization. Here, large numbers of resources from both authorized and unauthorized users are presented. A security is the most important problem in cloud computing for controlling the data access from the unauthorized users. In cloud environment, data owners and cloud service providers are required to ensure all data access activities to avoid unauthorized access. Through the key matching process, unauthorized users in the cloud are identified. While providing the access control, higher cloud security is ensured.

The cloud server and authentication server are utilized to obtain secured data outsourcing. All cloud users are registered at first for transmitting cloud data among cloud users and server in a secured manner. Here, encryption keys, tokens and decryption process are carried out to provide the data to different groups. After registering cloud user details, secured communication to user groups is provided. The private secrete keys for encryption are generated for data outsourcing. Then, the generated keys are stored in some data files to provide secured communication between cloud service provider and cloud users. Anonymous keys and cloud data authentication are performed to provide higher security in cloud environment.

Authentication plays an essential role in cloud computing security for verifying the user identity. In order to protect the resources which are stored in the cloud server from unauthorized user, an authentication is needed. Thus, enhanced data security in

cloud is attained by using biometrics-based authentication scheme. Biometrics technology uses the unique characteristics of cloud users to distinguish them from one another to ensure that the services are accessed only by an authorized user. But, the authentication performance of conventional multifactor authentication technique was poor where client's sensitive information is highly intrusive.

2. LITERATURE REVIEW

Authentication of cloud user data plays a fundamental component in cloud computing security. It is mainly utilized for accessing the cloud user data. Here, cloud computing services are presented by cloud service providers. In order to preserve the cloud user data stored in the cloud server from unauthorized user, authentication is required. Thus, many research work have been developed based on the authentication through anonymous keys.

Most of the existing techniques are designed for authentication in cloud environment. A K-Times Attribute-Based Anonymous Access Control was intended by Yuen et al. [1] to authenticate cloud user from the cloud computing server anonymously. In order to access the cloud user data within the time interval, a k-times limit is provided for anonymous access control. But, performance of anonymous access control was not sufficient.

An Identity Based Secure Authentication Scheme was developed by Sharma and Kalra [2] using quantum key distribution for improving security of cloud against attacks. With the identification of authorized cloud user, legitimate user gets access to the service and helps to attain sensitive information. However, authentication accuracy remained unsolved. Forward Secure ID-Based Ring Signature was introduced by Huang et al. [3] to attain efficient authentic and anonymous data sharing in cloud. The secured data sharing is achieved by providing a secret key. However, the secured data access is still remained unaddressed.

Message Digest-Based Authentication (MDA) was presented by Dey et al. [4] for obtaining enhanced authentication accuracy. With the utilization of hashing function with user ID and passwords, mutual authentication of cloud user data is

attained. But cloud data confidentiality rate is remained unaddressed. A Shared Authority-Based Privacy-Preserving Authentication Protocol (SAPA) was developed by Liu et al. [5] to address the privacy issues in cloud storage. Here, attribute-based access control is supported to recognize cloud data access and proxy re-encryption is applied to present data sharing among the multiple users. However, time taken for privacy-preserving authentication was more.

A Secure Elliptic Curve Cryptography Based Mutual Authentication Protocol was presented by Kalra and Sood [6] for achieving mutual authentication. By using Hyper Text Transfer Protocol, secured communication of embedded devices and cloud servers are achieved. Amin et al. [7] introduced a Light Weight Authentication Protocol to attain secured access of cloud data. In addition, informal cryptanalysis authenticates secured access of confidential data from any private cloud server. Thus, it attains higher data confidentiality but data integrity is low.

An enhanced user authentication framework was introduced by Cheng et al. [8] to avoid prohibited cloud users from requesting data information stored in a cloud environment. The time taken for accessing cloud data was higher. In order to access the cloud user's data with minimum time and computational cost, Server-Aided Anonymous Attribute-Based Authentication was designed by Liu et al. [9]. Accordingly, a Secured Authentication System was intended by Kim and Moon [10] to provide better performances of cloud data confidentiality, integrity and availability. But authentication performance was not effectual.

Biometrics-based Authentication Scheme was developed by Kumari et al. [11] with the use of authentication scheme, the users can easily access the data from any server. But it fails to improve the authentication accuracy. Therefore, various Multitier Authentication Methods were introduced by Singh and Singh [12] for accessing the data from cloud server. But various multitier authentication methods consume more time to recognize the authenticated user. An Efficient Revocable Attribute-Based Encryption scheme was developed by Xu et al. [13] for fine-grained access control and data sharing system. The scheme does not perform the authentication to obtain high security.

Selvarani et al. [14] developed a Hybrid Genetic Algorithm and Particle Swarm Optimization Algorithm to attain secured data authentication. This provides a secured and optimal authentication in cloud management. It consists of unauthorized user's accesses and it does not improve the cloud data confidentiality. In order to avoid unauthorized user's accesses of cloud data in cloud environment, Security Biometric Authentication Method was developed by Choi et al. [15] the method failed to use verification techniques for solving the security-usability trade-off.

A Privacy-Aware Access Control Approach was introduced by Lin et al. [16] for improving the cloud data security. The identification of authorized user access of cloud data is failed due to insufficient authentication mechanism. Thus, the authorized user access of data is obtained using Rijndael Encryption Algorithm developed by Singla and Singh [17]. It permits the authorized user accesses of data from the cloud server. The designed algorithm improves the security but the authentication was not performed effectively.

The secured outsourced data were achieved using developed Rule-Based Access Control Method by Wang et al. [18]. Here, secured data access is presented by allowing the authorized user to access data. But it failed to perform biometric authentication for obtaining higher data security. A Secured Anonymous Three-Factor Based Remote User Authentication Method was introduced by Chandrakar and Om [19] using Elliptical Curve Cryptography. It accesses cloud data effectively from cloud server but failed to provide better security in a cloud environment.

A Reputation-Based Identity Management Approach was presented by Wu et al. [20] for cloud computing. It identifies the malicious user while accessing data in secured manner. However, the access control mechanism was not used to improve the security in cloud computing. A Privacy-Aware Authentication Scheme was developed by Tsai and Lo [21] to minimize authentication processing time between cloud service providers and traditional trusted third-party service. But authentication performance was not effectual.

A Secured and Effective Two-Factor Remote User Authentication method was introduced by Chandrakar and Om [22] for achieving the mutual authentication. Here,

symmetric session key does not establish between a user and server for improving the secure communication. Chattaraj et al. [23] develop a New Dynamic Password-Based Two-Server Authentication and Key Agreement Protocol for data accessing. With the help of both public and private key cryptography, the secured cloud services for cloud data accessing were presented. But it failed to provide better security and performance in a real-world deployment.

An Efficient User Authentication Method was developed by Zhao et al. [24] for improving the secured communication and computation efficiency. It does not use any hash function. Thus, it failed to improve the security in the cloud data accessing. Trust Enhanced Cryptographic Role-Based Access Control was designed by Wu et al. [25] for secured cloud data storage. However, confidentiality of data was remained unaddressed.

A key-Aggregate Cryptosystem was designed by Guo et al. [26] with the goal of attaining secure data sharing in dynamic cloud storage. But computational complexity was very higher. A Modified Smart Card-Based Verification Scheme was presented by Li et al. [27] for secured communication in cloud environments. But, the identification of correctly accessed data for data communication by user is lower.

An Authorized Accessible Privacy Model was designed by Zhou et al. [28] to increase security and privacy in the cloud. The unauthorized user is determined by satisfying the data access using personal health information. However, the computational and communication overhead was higher. An Identity-Based Remote Data Integrity Checking Protocol was introduced by Yu et al. [29] to minimize the complexity and cost of public key verification. With the use of key-homomorphism cryptographic techniques, privacy-preserving rate is not enhanced.

Cloud-Assisted Mutual Authentication and Privacy Preservation Protocol were presented in Tali et al. [30] to attain improved security. The authenticated user improves the secured data communication. But, time for user authentication is high. A Secured Disintegration Protocol (SDP) was introduced by Rawal et al. [31] for the safeguard the privacy on-site in the cloud. However, secured data integration was not solved.

Liu et al. [32] developed a Two-Factor Data Security Protection Mechanism for cloud storage. The public key is generated for encrypting and decrypting the data in cold storage. But the time required for authenticating the users in the cloud was very higher. Mutual Authentication Protocol was introduced by Kumar et al. [33] for reducing the data communication cost. With aid of secured elliptic curve cryptography, minimum communication cost is attained. However, privacy-preserving rate was minimal.

A Handoff Authentication Scheme with security and privacy was presented by Yang et al. [34] for providing user anonymity and untraceability in the cloud. Reddy et al. [35] presented a Privacy-Preserving Three-Factor Authenticated Key Agreement Protocol. It attains a secured data from various attacks with higher security in the cloud. A novel technique was intended by Dhasarathan et al. [36] for Secured Data Privacy Preservation in On-Demand Cloud Services. But, authentication performance of conventional authentication technique was not addressed effectively.

Several issues have been discovered from the above reviews such as less authentication accuracy, more authentication time, lack of confidentiality, and so on. In the proposed research work, the above said issues related to secured cloud data accessing are addressed by the implementation of three techniques such as Threshold ElGamal Cryptosystem Based Anonymous Key Authentication (TEC-AKA) technique, Tiger Hash-Based Kerberos Biometric Blowfish Authentication (TH-KBBA) Mechanism, and Suppressed k-Anonymity Multi-Factor Authentication Based Schmidt-Samoa Cryptography **(**SKMA-SC) technique.

3. OBJECTIVES

The major objectives of this research work are

- To improve the performance of authentication with secured cloud data accessing, confidentiality and integrity of data, encryption and decryption are performed.
- To enhance the accuracy of cloud user authentication with less time consumption, Cryptographic Hash Function and Symmetric Key Cryptography are implemented.
- To enhance the security and data privacy-preservation of cloud service, suppression method, multifactor authentication process, encryption and decryption are performed.

4. RESEARCH PROBLEM

The main focus of our research problem is, to perform secured data access with higher accuracy in cloud environment with less time consumption and enhanced protection and data privacy-preservation of cloud services. In order to achieve our research focus, we have proposed the following authentication techniques.

4.1 Threshold ElGamal Cryptosystem Based Anonymous Key Authentication

A Threshold ElGamal Cryptosystem based Anonymous Key Authentication (TEC-AKA) technique is proposed for improving the security of data access in cloud. The main purpose of developing proposed TEC-AKA technique is to obtain secured data access with higher data confidentiality and integrity. This is achieved with different processes such as Registration phase, User ID and Anonymous Key generation, Authentication Server, Threshold ElGamal Encryption and Threshold ElGamal Decryption. Initially, registration phase is performed to register the user's details on cloud server efficiently to perform authentication process. Here, registration is carried out by transmitting the user's request to the cloud server and all the transmitted data are stored in cloud server. After completing registration phase, user

ID and anonymous key generation are done to generate individual user ID and key for each user. The generated user identity helps to identify and distinguish between the users. Followed by, public key and private key improve the cloud data security. Next, the authenticity of user is verified by the authentication server. The authentication server authenticates the identity of user who requests the cloud service by using Kernelized binary classifier. Then, Threshold Elgamal Encryption is performed before transmitting cloud data to users to improve the privacy preservation and obtaining high data security. Here, cloud server renders the user required data in an encrypted format with the support of server public key. Finally, threshold Elgamal Decryption is performed at the receiver side for obtaining original data with their private key. The user can decrypt the cipher text and threshold. Therefore, proposed TEC-AKA technique improves the performance of secured data access in cloud.

Threshold ElGamal Encryption Algorithm

The Threshold ElGamal Encryption Algorithm described below can be used for encrypting the data for secured data access.

Input: Cloud Data '$D_i = D_1, D_2, \ldots D_n$', random number '$k$', public key '$PK_i$'.

Output: Cipher Text

Step 1: for every D_i

Step 2: Choose random number 'k'

Step 3: The cloud data D_i is encrypted with public key 'PK_i', random number 'k' and using $CT_1 = g^k \ (mod\ Pr)$ and $CT_2 = D\ xor\ PK_i{}^k$

Step 4: Threshold 't' is set to allow number of users to decrypt the encrypted data using $t = \delta,\ where\ \delta < n$

Step 5: end for

Step 6: end

Threshold ElGamal Decryption Algorithm

The Threshold ElGamal Decryption Algorithm described below can be used for decrypting the data for secured data access.

Input: Cipher Text '$C_i = C_1, C_2, \ldots C_n$', Public Key '$PK_i$' and Private Key '$SK_i$', Threshold '$t$'

Output: Original Cloud Data

Step 1: for each received Cipher Text C_i

Step 2: Anonymous key authentication is performed using

$$= \begin{cases} If\ (PK_S == PK_R), then\ decryption\ is\ allowed \\ else\ then\ decryption\ is\ declined \end{cases}$$

Step 3: If public key of both sender and receiver is matched and $t \leq \delta$, then

Step 4: The decryption process is performed to obtain original data using

$$D = \left(CT_1{}^{SK_i}\ mod\ Pr\right) xor\ CT_2\ \ if\ and\ only\ if\ t \leq \delta.$$

Step 5: else

Step 7: The decryption process is declined

Step 8: end if

Step 9: end for

Step 10: end

4.2 Tiger Hash-Based Kerberos Biometric Blowfish Authentication Mechanism

Tiger Hash-Based Kerberos Biometric Blowfish Authentication (TH-KBBA) mechanism is designed for accessing data from server with improved authentication accuracy. With the consideration of different entities such as number of users, authenticate server and cloud server, secured data accessing is performed. The proposed TH-KBBA mechanism is designed using three different phases namely Registration Phase, Authentication phase and Ticket Granting phase. At first, registration phase is performed on cloud user to register the details for accessing data in a secured manner. For each cloud user, details are entered such as name, first name,

last name, age, date of birth and so on. Here, tiger hash function is utilized to generate hash value for each user data and user information is stored in cloud server. While cloud user registration is presented, user ID and password are given by cloud server. After registering cloud user details based on ID and password, Biometric authentication phase is performed. When client wants to access data from server, authentication server verifies user identity by sending a message. Based on the authentication process, authorized user is identified to access the cloud data with higher security and authentication accuracy. Finally, tickets are generated for each authenticated user in cloud server. By using Blowfish encryption process, the authentication server generates a ticket and encrypts the ticket. Then, the server decrypts the ticket using blowfish decryption technique and verifies the user ID. If two users IDs get matched, then the cloud server offers requested data to the user. Hence, proposed TH-KBBA mechanism ensures security level with higher data confidentiality rate. The following algorithm, can be used for identifying the authenticated users with less time.

Algorithm

Input: Number of cloud users $CU = CU_1, CU_2, \ldots . CU_n$, data

$D_1, D_2, D_3, \ldots . D_n$

Output: Secured data access in the cloud

Step 1: For each CU_i

Step 2: Send user information to CS

Step 3: CS stored information with hash value $f(x)$

Step 4: U_i login with $User_ID$ and BK

Step 5: if $BK = BK_{cs}$ then

Step 6: User is said to be an authenticated

Step 7: else

Step 8: User is said to be an unauthorized

Step 9: end if

Step 10: S_A generates a ticket (T)

Step 11: Encrypt ticket into ciphertext (C) with SK

Step 12: S_A send C into user CU_i

Step 13: CU_i sends C with User_ID to CS

Step 14: CS decrypts T with SK

Step 15: If $(\mathrm{ID_a} = ID)$ then

Step 16: CS grants the requested data to CU_i

Step 17: else

Step 18: CS denied the services to CU_i

Step 19: end if

Step 20: end for

Step 21: end

4.3 Suppressed K-Anonymity Multi-Factor Authentication Based Schmidt-Samoa Cryptography Technique

A Suppressed K-Anonymity Multi-Factor Authentication Based Schmidt-Samoa Cryptography **(**SKMA-SC) technique is proposed finally to avoid the unauthorized access of cloud data and achieving higher data privacy preservation in the cloud computing. The SK-AMFA technique is proposed by using three various key processes namely registration phase, authentication phase and data access phase. For enhanced performance of data accessing, request from clients is transmitted to the cloud server. The cloud user identification information's are registered at first during the registration phase. With the support of suppression method, registered details are securely stored in cloud server. With the privacy preservation of client identification

details, the verification performance of users is enhanced in the cloud. This helps to preserve the client sensitive information's from adversaries or third parties. After registration of client details, the authentication phase is performed by considering multifactor such as password, one-time token and conditional attributes. The considered multifactor authenticates the identity of clients. The user authentication performance is enhanced with the aid of one-time token in cloud with higher accuracy. Finally, data access phase is carried out to provide the required cloud data services for authorized person in cloud environment. The authorized persons are only allowed to get requested data services through the performance of Schmidt-Samoa data encryption/decryption process. This helps to avoid illegal access from unauthorized party over insecure communications in a cloud environment with a lower amount of time. Thus, enhanced performances of authentication are attained with minimum time.

Algorithm

Input: Number of Clients '$C = C_1, C_2, \ldots . C_n$',

Output: Privacy preserved data access in the cloud

Step 1: For each client 'C_i'

Step 2: For each client person details

Step 3: Generate '*Cid'* and 'PWD' using $CS \rightarrow Cid, PWD$

Step 4: Set conditional attributes 'CA' using $C_{id} \rightarrow (CA_1, CA_2, .. CA_n)$

Step 5: Store 'PWD' and 'CA' in cloud server database using suppression method

Step 6: Cloud server issue ' C_{id}' and 'PWD' to client

Step 7: End for

Step 8: For client login with 'C_{id}' and 'PWD'

Step 9: Cloud server Generate 'OTT' and sent it to 'C_i' using $Cid \rightarrow OTT$ and $OTT = \{r\}$

Step 10: If (($PWD = PWD^*$) && ($OTT = OTT^*$) && ($CA = CA^*$))

Step 11: 'C_i' is an authentic

Step 12: else

Step 13: 'C_i' is an unauthentic

Step 14: Endif

Step 15: If (client 'C_i' is authroized), then

Step 16: 'C_i' is permitted to obtain needed data services by carried out by using Schmidt-Samoa data encryption/decryption

Step 17: else

Step 18: 'C_i' is not allowed to get the required data services

Step 19: Endif

Step 20: End for

Step 21: End for

Step 22: End

5. ORGANIZATION OF THESIS

Chapter 1, "Introduction" presents a brief introduction to cloud computing and to access the cloud data in a secure manner. It also discusses the state-of-the-art methods of authentication techniques to secure sensitive information against adversaries in cloud environment, privacy-preservation techniques are given in detail. A discussion on Anonymous Authentication, Biometric Authentication and Multifactor Authentication is also given. This chapter also outlines motivation, objectives, contribution and organization of thesis.

Chapter 2, "Literature Survey", describes literature survey on reviews the previous work done in the field of authentication scheme to check all data access activities to avoid unauthorized access. This chapter also reviews the existing literatures over Anonymous Access Control Scheme, Biometrics and Identity-Based Authentication Scheme, PriGuarder and Attribute Based Signature Outsourcing Protocol.

Chapter 3, "Threshold ElGamal Cryptosystem Based Anonymous Key Authentication" technique presents a secured data access with higher data

confidentiality and Integrity. This technique is employed with different phases such as Registration phase, User ID and Anonymous Key generation, Authentication Server, Threshold ElGamal Encryption and Threshold ElGamal Decryption. The performance of the proposed algorithm is analyzed by considering the Authentication Accuracy, Authentication Time, Data Confidentiality and Data Integrity rate. The Results are analyzed and discussed.

Chapter 4, "Tiger Hash-Based Kerberos Biometric Blowfish Authentication" is introduced for improving the authentication accuracy with minimal authentication time for accessing data from server. The mechanism is developed by using three different steps such as Registration step, Authentication step and Ticket generation step. The proposed mechanism is verified by conducting the experiments with parameters such as Authentication Accuracy, Authentication Time, Data Confidentiality. The Results are analyzed and discussed.

Chapter 5, "Suppressed K-Anonymity Multi-Factor Authentication Based Schmidt-Samoa Cryptography" presents a technique to improve security and data privacy-preservation of cloud services. This technique includes three main processes namely Registration phase, Authentication phase and Data Access phase. The performance is evaluated using the metrics Authentication Accuracy, Authentication time and Privacy Preserving Rate. The Results are analyzed and discussed.

Chapter 6, presents the analysis on Threshold ElGamal Cryptosystem Based Anonymous Key Authentication technique, Tiger Hash-Based Kerberos Biometric Blowfish Authentication mechanism and Suppressed K-Anonymity Multi-Factor Authentication Based Schmidt-Samoa Cryptography technique with different parameters.

Chapter 7, concludes by summarizing the research work done and provides discussions for future work in this area.

REFERENCES

1. T. H. Yuen, J. K. Liu, M. H. Au, X. Huang, W. Susilo and J. Zhou, k-times Attribute-Based Anonymous Access Control for Cloud Computing, *IEEE Transactions on Computers*, **64** (9) (2015), 2595 – 2608.
2. G. Sharma and S. Kalra, Identity Based Secure Authentication Scheme Based on Quantum Key Distribution for Cloud Computing, *Peer-to-Peer Networking and Applications*, **11** (2) (2018), 220–234.
3. X. Huang, J. K. Liu, S. Tang, Y. Xiang, K. Liang, L. Xu and J. Zhou, Cost-Effective Authentic and Anonymous Data Sharing with Forward Security, *IEEE Transactions on Computers*, **64** (4) (2015), 971 – 983.
4. S. Dey, S. Sampalli and Q. Ye, MDA: Message Digest-Based Authentication for Mobile Cloud Computing, *Journal of Cloud Computing: Advances, Systems and Applications*, **5** (18) (2016), 1-13.
5. H. Liu, H. Ning, Q. Xiong, and L.T. Yang, Shared Authority Based Privacy-Preserving Authentication Protocol in Cloud Computing, *IEEE Transactions on Parallel and Distributed Systems*, **26** (1) (2015), 241 – 251.
6. S. Kalra and S. Sood, Secure Authentication Scheme for IOT and Cloud Servers, *Pervasive and Mobile Computing*, **24** (2015), 210-223.
7. R. Amin, N. Kumar, G. P. Biswas, R. Iqbal and V. Chang, A Light Weight Authentication Protocol for IOT-Enabled Devices in Distributed Cloud Computing Environment, *Future Generation Computer Systems*, **78** (3) (2018), 1005-1019.
8. L. Cheng, D. M. Divakaran, A. W. K. Ang, W. Y. Lim and V. L. Thing, FACT: A Framework for Authentication in Cloud-Based IP Trace Back, *IEEE Transactions on Information Forensics and Security*, **12** (3) (2017), 604 – 616.
9. Z. Liu, H. Yan and Z. Li, Server-Aided Anonymous Attribute-Based Authentication in Cloud Computing, *Future Generation Computer Systems*, **52** (1) (2015), 61-66.

10. J. Kim and J. Moon, Secure Authentication System for Hybrid Cloud Service in Mobile Communication Environments, *International Journal of Distributed Sensor Networks*, **2014** (2014), 1-7 Article Id 828092.
11. S. Kumari, X. Li, F. Wu, A. K. Das, K. Kwang, R. Choo and J. Shen, Design of a Provably Secure Biometrics-Based Multi-Cloud-Server Authentication Scheme, *Future Generation Computer Systems*, **68** (2017), 320–330.
12. M. Singh and S. Singh, Design and Implementation of Multi-Tier Authentication Scheme in Cloud, *International Journal of Computer Science*, **9** (5) (2012), 181-187.
13. S. Xu, G. Yang, Y. Mu and R. H. Deng, Secure Fine-Grained Access Control and Data Sharing for Dynamic Groups in the Cloud, *IEEE Transactions on Information Forensics and Security*, **13** (8) (2018), 2101 – 2113.
14. P. Selvarani, A. Suresh and N. Malarvizhi, Secure and Optimal Authentication Framework for Cloud Management Using HGAPSO Algorithm, *Cluster Computing*, **22** (9) (2019), 1-10.
15. Y. Choi, Y. Lee, J. Moon and D. Won, Security Enhanced Multi-Factor Biometric Authentication Scheme Using Bio-Hash Function, *PLoS ONE*, **12** (5) (2017), 1-32.
16. L. Lin, T. T. Liu, S. Li, C. M. S. Magurawalage and S. Tu, PriGuarder: A Privacy-Aware Access Control Approach Based on Attribute Fuzzy Grouping in Cloud Environments, *IEEE Access*, **6** (2017), 1882 – 1893.
17. S. Singla and J. Singh, Cloud Data Security Using Authentication and Encryption Technique, *International Journal of Advanced Research in Computer Engineering and Technology*, **2** (7) (2013), 2232- 2235.
18. H. Wang, X. Yi, E. Bertino and L. Sun, Protecting Outsourced Data in Cloud Computing Through Access Management, *Concurrency and Computation: Practice and Experience*, **28** (3) (2014), 1-16.
19. P. Chandrakar and H. Om, A Secure and Robust Anonymous Three-Factor Remote User Authentication Scheme for Multi-Server Environment Using ECC, *Computer Communications*, **110** (2017), 26-34.

20. L. Wu, S. Zhou, Z. Zhou, Z. Hong and K. Huang, A Reputation-Based Identity Management Model for Cloud Computing, *Mathematical Problems in Engineering*, **2015** (1) (2015), 1-15.
21. J. Tsai and N. Lo, A Privacy-Aware Authentication Scheme for Distributed Mobile Cloud Computing Services, *IEEE Systems Journal*, **9** (3) (2015), 805-815.
22. P. Chandrakar and H. Om, RSA Based Two-factor Remote User Authentication Scheme with User Anonymity, *Procedia Computer Science*, **70** (2015), 318-324.
23. D. Chattaraj, M. Sarma and A. K. Das, A New Two-Server Authentication and Key Agreement Protocol for Accessing Secure Cloud Service, *Computer Networks*, **131** (2018), 144-164.
24. Y. Zhao, S. Li and L. Jiang, Secure and Efficient User Authentication Scheme Based on Password and Smart Card for Multi Server Environment, *Security and Communication Networks*, **2018** (2018), 1-13.
25. X. Wu, R. Jiang and B. Bhargava, On the Security of Data Access Control for Multiauthority Cloud Storage Systems, *IEEE Transactions on Services Computing*, **10** (2) (2017), 258 – 272.
26. C. Guo, N. Luo, M. Z. A. Bhuiyan, Y. Jie, Y. Chen, B. Feng and M. Alam, Key-Aggregate Authentication Cryptosystem for Data Sharing in Dynamic Cloud Storage, *Future Generation Computer Systems*, **84** (2018), 190-199.
27. X. Li, J. Niu, M. K. Khan and J. Liao, An Enhanced Smart Card Based Remote User Password Authentication Scheme, *Journal of Network and Computer Applications*, **36** (2013), 1365–1371.
28. J. Zhou, X. Lin, X. Dong and Z. Cao, PSMPA: Patient Self-Controllable and Multi-Level Privacy-Preserving Cooperative Authentication in Distributed M-Healthcare Cloud Computing System, *IEEE Transactions on Parallel and Distributed Systems*, **26** (6) (2015), 1693 – 1703.

29. Y. Yu, M. Au, G. Ateniese, X. Huang, W. Susilo, Y. Dai and G. Min, Identity-Based Remote Data Integrity Checking with Perfect Data Privacy Preserving for Cloud Storage, *IEEE Transactions on Information Forensics and Security*, **12** (4) (2017), 767 – 778.

30. C. Tali, D. Hershih and C. Wang, Cloud-Assisted Mutual Authentication and Privacy Preservation Protocol for Telecare Medical Information Systems, *Computer Methods and Programs in Biomedicine*, **157** (2018), 191-203.

31. B. S. Rawal, V. Vijayakumar, G. Manogaran, R. Varatharajan and N. Chilamkurti, Secure Disintegration Protocol for Privacy Preserving Cloud Storage, *Wireless Personal Communications*, **103** (1) (2018), 1–17.

32. L. Joseph, L. Kaitai, S. Willy, L. Jianghua and X. Yang, Two-Factor Data Security Protection Mechanism for Cloud Storage System, *IEEE Transactions on Computers*, **65** (6) (2016), 1992-2004.

33. V. Kumar, M. Ahmad and A. Kumari, A Secure Elliptic Curve Cryptography Based Mutual Authentication Protocol for Cloud-Assisted TMIS, *Telematics and Informatics*, **38** (2018), 1–21.

34. X. Yang, X. Huang and J. K. Liu, Efficient Handover Authentication with User Anonymity and Untraceability for Mobile Cloud Computing, *Future Generation Computer Systems*, **62** (2016), 190-195.

35. A. Reddy, A. Das, V. Odelu, A. Ahmad and J. Shin, A Privacy-Preserving Three-Factor Authenticated Key Agreement Protocol for Client-Server Environment, *Journal of Ambient Intelligence and Humanized Computing*, **10 (**2018), 1–17.

36. C. Dhasarathan, V. Thirumal and D. Ponnurangam, A Secure Data Privacy Preservation for On-Demand Cloud Service, *Journal of King Saud University - Engineering Sciences*, **29** (2) (2017), 144-150.

LIST OF PUBLICATIONS

1. K. Mohana Prabha and P. Vidhya Saraswathi, Threshold Elgamal Asymmetric Cryptography based Anonymous Key Authentication for Secured Cloud Data Access, *Journal of Advanced Research in Dynamical and Control Systems*, **18** (8) (2018), 678-688.
2. K. Mohana Prabha and P. Vidhya Saraswathi, Tiger Hash Kerberos Biometric Blowfish User Authentication for Secured Data Access in Cloud, *Proceedings of the Second International conference on I-SMAC*, (2018), 145-151.
3. K. Mohana Prabha and P. Vidhya Saraswathi, Secured Mobile Cloud Service System Based on Trapdoor, *International Journal of Innovative Technology and Exploring Engineering*, **9**, (2019), 772-775.
4. K. Mohana Prabha and P. Vidhya Saraswathi, Suppressed K-Anonymity Multi-Factor Authentication Based Schmidt-Samoa Cryptography for Privacy Preserved Data Access in Cloud Computing, *Computer Communications*, **158** (2020), 85-94.
5. K. Mohana Prabha, P. Vidhya Saraswathi and S. Balamurali, Tversky Anonymous Key Authentication Based Blum Goldwasser Cryptography for Cloud Data Access Security, *Turkish Online Journal of Qualitative Inquiry*, **12** (5) (2021*)*, 257– 1271.
6. K. Mohana Prabha, P. Vidhya Saraswathi and S. Balamurali, Whirlpool Hash Mutual Biometric Serpent Authentication for Secured Data Access in Cloud Environment, *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, **22** (2) (2022), 72-80.